The Haunted Lighthouse Limited

Security & Compliance Overview
v1.0

1. Overview

The Haunted Lighthouse Limited incorporates industry-aligned security practices across all deployments. Our consultancy and hosted services prioritise privacy, EU sovereignty, data minimisation, and operational resilience. This document outlines our core security stance and compliance model.

2. Security Principles

- Least-privilege access across all systems
- Encrypted storage and encrypted backups
- Strong authentication (TOTP/WebAuthn for admin roles)
- TLS enforced across public endpoints
- No reliance on Cloudflare or non-EEA CDNs
- Traffic flows restricted via firewalls and service isolation

3. Infrastructure Security

- Bare-metal hosting within the EEA (primarily HEL1)
- Hardened OS configurations
- Regular package and kernel updates
- Service isolation via systemd, containers, or both
- SSH key-based access only (no password logins)
- Optional IP restriction for administrative endpoints

4. Data Protection & GDPR Alignment

- Data stored exclusively on EEA infrastructure
- Backups encrypted using strong cryptography
- Optional data-processing agreements (DPAs) available
- No transmission to third-country processors
- Data minimisation practices integrated by design

5. Backup & Recovery Security

- Nightly encrypted backups for all managed services
- Off-site encrypted retention
- Verified backup integrity checks
- Defined disaster recovery workflow
- Controlled restoration on compliant EU hardware

6. Monitoring & Incident Response

- Active service monitoring and health checks
- Optional alerting via Telegram or email
- Manual review of logs and critical event patterns
- Defined incident response procedures

7. Client Responsibilities

- Maintain secure client-side access devices
- Protect administrative accounts with TOTP/WebAuthn
- Follow provided guidelines for moderation and account roles
- Notify The Haunted Lighthouse Limited of suspected breaches

8. Next Steps

Clients seeking enhanced security reviews or policy development can request:

- Platform-specific risk assessments
- GDPR guidance for self-hosted deployments
- Backup and DR alignment reviews
- Documentation and policy creation

9. Contact
contact@haunted.lighthouse.co.im
https://haunted.lighthouse.co.im/consultancy